Tip of the Month – January 2011

FRAUD PREVENTION IN BANKING

The ability to control how your personal information is collected and used is the essence of privacy. Personal information in the wrong hands could be used to carry out different financial crimes ranging from debit and credit card fraud to email scams and real estate fraud. Identity theft is also a real possibility. Make sure the bank you frequent have dedicated privacy officers who ensure that their customers' information is being protected.

A good bank will have several guiding principles to follow when dealing with your personal information including:-

Ensuring individuals understand why information is being collected before it is collected

Obtaining customers' consent regarding the collection, use or disclosure of this information

Using information only for the purpose for which it has been collected and for which consent was granted

Providing customers with access to the information held about them and allowing customers to amend or correct their personal information.

Working to protect you- online and off

Banks work hard to protect the information they have about you, and you should too. Both online and off, savvy criminals are watching for you to let your guard down and unintentionally provide access to personal data that can be used to steal your money or commit financial fraud.

Today, the Internet lets you shop, bank, and even interact with friends around the world, all from the comfort of your own home. And because it is so easy and convenient, people often get lulled into a false sense of security. The unfortunate reality is that as Internet use grows, the number of criminals who use online means to commit crimes is also growing.

When using the Internet it is important to safeguard your personal information. Here are some steps you can take to ensure your personal information is secure.

When online, know who you're dealing with and be aware of potential security leaks. You wouldn't give information to just anyone in the off-line world, apply the same common-sense discretion online.

Change your password regularly, use hard-to-guess passwords (e.g. using a combination of letters and numbers), and never share your password with anyone-not even close family.

Install and frequently update proven anti-virus software and also maintain a firewall to guard against unwanted access to your computer.

Look for a company's privacy policy or link to its privacy statement when you visit its website. Pay attention to what information the company gathers, how it's used, and with whom it's shared.

Use caution if you receive e-mail from a business or person requesting information or directing you to websites that request your password, National Insurance Number or other highly sensitive information. If unsure of the legitimacy of a request, call the organization for verification.

When using social networking sites, limit the information you share publicly, avoid posting your phone number, address or birth date and only accept friend requests from people you know.

File sharing websites are popular with online criminals and should be avoided. Legitimate downloading sites have security measures in place to protect your personal data and are a much safer option.

Invest in a Shredding Machine

The Internet isn't the only place criminals can access unguarded personal information; they may also be able to find valuable data at your dumpster.

If you are like most people, each week you probably throw away numerous bills, letters, financial statements and other documents containing personal information. A criminal can easily rummage through your garbage bin for an old bank statement or credit card bill and gather your personal information.

Luckily there is an easy way to protect yourself: shred all documents containing personal information before they are put into the recycling bin. Personal shredders are easy to use, inexpensive and widely available at office supply and department stores across the country. Shredding documents before you recycle them will go a long way to ensure you do not become a victim of identity theft or financial fraud.

Below is a list of documents that should be shredded before they go out to the curb:-

Financial statements from your bank or investment advisor

Bills from phone companies, credit cards and cable and Internet providers

Expired credit cards, insurance claims and old prescription forms.